

Privacy Policy of the Ontario Party

Publication of the Policy

Once accepted by Elections Ontario, the Privacy Policy of the Ontario Party shall be published on the official Ontario Party website (ontarioparty.ca) within 30 days of receiving an acceptance confirmation from Elections Ontario.

Section 1: Scope of Policy

Pursuant to Section 17.6 of the Election Act, political entities accessing electors' personal information held by Elections Ontario must develop and implement a privacy policy. The Ontario Party establishes the following Privacy Policy to govern the use, storage, and secure disposal of any List Products provided by Elections Ontario, including but not limited to the Permanent and Absentee Registers.

This Privacy Policy applies to all staff, volunteers, representatives, agents, and associates of the Ontario Party, as well as any vendors or suppliers with access to the List Products.

Section 2: Restriction on Use

As per Section 17.4 of the Election Act:

1. Definition of "The Data"

For the purposes of this policy, *The Data* refers to all List Products provided by Elections Ontario, including voter information obtained from the Permanent and Absentee Registers.

2. Permitted Uses

The Data shall be used strictly for electoral purposes, which include:

- Communicating with voters.
- Soliciting campaign support, including donations and volunteer recruitment.
- Administering the distribution of campaign signs.

- Identifying and engaging with potential supporters.
- Election-day voter outreach and Get-Out-The-Vote (GOTV) efforts.

3. Access Control & Tracking

- Only authorized individuals shall access *The Data*.
 - Distribution and access shall be centrally tracked and controlled by the Chief Privacy Officer (CPO) using Elections Ontario Forms F0101 and F0315 (or functional equivalents).
 - All individuals accessing *The Data* must complete Form F0101 before authorization is granted.
-

Section 3: Privacy Requirements

3.1 Implementation and Enforcement of Privacy Controls

To ensure full compliance with Elections Ontario privacy and security requirements, the following controls are implemented:

a) Physical Controls

- Hard copies of *The Data* shall be stored in locked filing cabinets or secured rooms with limited access.
- Only authorized personnel may retrieve or handle printed voter information.
- Computers and other electronic devices used to store *The Data* shall be kept in secure/locked locations when not in use.
- Any computers used to access *The Data* must require multi-factor authentication (MFA).
- If *The Data* is stored on removable media (e.g., flash drives, external hard drives), it shall be encrypted using industry-standard encryption protocols.
- All removable storage devices shall be kept in a secure location when not in use.

b) Administrative Controls

- Access to *The Data* shall be granted on a strictly “need to know” basis, as determined by the Chief Privacy Officer (CPO) or their duly appointed deputies.
- Individuals requesting access shall be assessed for suitability in handling sensitive voter information.
- The CPO shall maintain audit trails tracking who accessed *The Data*, when, and for what purpose.

c) Technical Controls

- *The Data* stored digitally shall be password-protected, encrypted, and monitored for unauthorized access.
- Audit trails and system logs shall be maintained to track any modifications or access attempts.
- Firewalls, encryption, and other modern IT security measures shall be implemented to safeguard *The Data*.
- Remote access to *The Data* shall be prohibited unless explicitly authorized by the Chief Privacy Officer.

3.2 Disposition Protocol for List Products

Upon completion of the electoral purpose for which *The Data* was accessed, the Ontario Party shall securely dispose of the information following Elections Ontario’s Secure Destruction of List Products requirements.

1. Digital Data Destruction

- Data shall be erased using Communication Security Establishment Canada (CSEC)-approved wiping methods to ensure that no personal information can be reconstructed.

2. Hard Copy Disposal

- Physical copies of *The Data* shall be cross-cut shredded (single-strip shredding is not permitted).

- Shredding shall occur immediately upon determination that *The Data* is no longer required.

3.3 Training on Privacy Controls

1. Training Format:

- Privacy training for individuals accessing *The Data* will be conducted in-person and/or virtually to accommodate all personnel.

2. Training Scope:

- Training sessions shall cover both the Ontario Party's Privacy Policy and Elections Ontario's Privacy Policy to ensure full compliance.
- All individuals must acknowledge, in writing, their understanding of the policies before accessing *The Data*.
- The Chief Privacy Officer (CPO) and/or their duly appointed deputies shall be responsible for carrying out the training.

Section 4: Breach Management

- Any accidental or unauthorized access, disclosure, modification, or disposal of *The Data* must be immediately reported to the Chief Privacy Officer (CPO).
- In the case of loss, theft, or unauthorized access, the Chief Privacy Officer shall:
 - Assess the scope of the breach.
 - Take immediate mitigation measures (e.g., revoking access, strengthening security controls).
 - Notify the Chief Electoral Officer of Elections Ontario as required.

Section 5: Roles and Responsibilities

Chief Privacy Officer (CPO):

The Ontario Party's Chief Privacy Officer is responsible for:

- Ensuring the safeguarding of electors' personal information against accidental or unauthorized access, disclosure, use, modification, and disposal.
- Complying with all Elections Ontario filing requirements.
- Overseeing the implementation, updating, and enforcement of this Privacy Policy.

Responsibilities of Individuals with Access

- All individuals authorized to access *The Data* must comply with this Privacy Policy.
- Individuals must immediately report any breaches or suspicious activity to the CPO.

Section 6: Privacy Policy Approval

This Privacy Policy is approved and signed by:

Chief Privacy Officer (CPO):



Thomas James Marazzo

Approval Date: 10 February 2025